



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/693,182	10/23/2003	Chris D. Hyser	200205371-1	2604
22879 7590 12/10/2007 HEWLETT PACKARD COMPANY P O BOX 272400, 3404 E. HARMONY ROAD INTELLECTUAL PROPERTY ADMINISTRATION FORT COLLINS, CO 80527-2400			EXAMINER ALMEIDA, DEVIN E	
			ART UNIT 2132	PAPER NUMBER
			NOTIFICATION DATE 12/10/2007	DELIVERY MODE ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

Office Action Summary

Application No.

10/693,182

Applicant(s)

HYSER, CHRIS D.

Examiner

Devin Almeida

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 11/05/2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-18 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-18 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

This action is in response to the papers filed 11/05/2007. Claims 1-18 were received for consideration. Currently claims 1-18 are under consideration.

Response to Arguments

Applicant's arguments with respect to Jones not teaching "a pair of data-storage media each containing a sequence of encryption keys, one data-storage medium local to the monitor, and the other data-storage medium local to the remote computer system" have been fully considered but they are not persuasive. Jones clearly teaches that both the transmitting station (computer device) and the receiving station (remote computer system) have a sequence of encryption key that that are changed at predetermined times (see figure 1 and abstract).

In response to applicant's arguments, the recitation "a monitor that monitors the security state of a remote computer system, the monitor comprising" has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneck et al (U.S. 6,865,426) in view of Jones (U.S. 5,412,730). With respect to claim 1, Schneck teaches a monitor that monitors the security state of a remote computer system, the monitor comprising: a computing device (see figure 1 element 106 Receive Host) and a communications medium interconnecting the computing device with the remote computer system (see figure 1 element 103 Send Host). Schneck teach using encrypted communication between the devices but does not teach a pair of data-storage media each containing a sequence of encryption keys, one data-storage medium local to the monitor, and the other data-storage medium local to the remote computer system; and a program, running on the computing device, that exchanges with the remote computer system, over the communications medium, messages encrypted using one or more encryption keys extracted from the data-storage medium local to the remote computer system in order to monitor the security state of the remote computer system. Jones teaches a pair of data-storage media each containing a sequence of encryption keys (see Jones figure 1 element 23 and 27), one data-storage medium local to the monitor (see Jones figure 1 element 27), and the other data-storage medium local to the remote computer system (see Jones figure 1 element 23 and 27 and abstract); and a program, running on the computing device, that exchanges with the

remote computer system, over the communications medium, messages encrypted using one or more encryption keys extracted from the data-storage medium local to the remote computer system in order to monitor the security state of the remote computer system (see abstract). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have a pseudo-random number generator at the transmitting and receiving stations to supply a like sequence of encryption keys to both the encryptor and decryptor, without these keys being transmitted in any form over the transmission facility. Therefore one would have been motivated to have a pseudo-random number generator at the transmitting and receiving stations to supply a like sequence of encryption keys to both the encryptor and decryptor (see column 1 lines 37-53).

With respect to claim 2, wherein following power on or reset of the remote computer system, while the remote computer system is in a relatively high-security state, the remote computer system sends an initial-authentication message to the monitor, encrypted with a next key extracted from the data-storage medium local to the remote computer system (see Schneck column 4 line 66 – column 5 line 24 and column 7 line 55 – column 9 line 12 and column 10 line 26 – 67).

With respect to claim 3, wherein the monitor receives the initial-authentication message, decrypts the initial-authentication message using a next key extracted from the data-storage medium local to the monitor, and stores an indication that the remote computer system is in a relatively high-security state (see Schneck column 4 line 66 – column 5 line 24 and column 7 line 55 – column 9 line 12).

With respect to claim 4, wherein the remote computer system collects security metrics and includes the security metrics in the initial-authentication message (see Schneck column 4 line 66 – column 5 line 24 and column 7 line 55 – column 9 line 12 and column 10 line 26 – 67).

With respect to claim 5, wherein the monitor receives the initial-authentication message and extracts the security metrics in order to determine the security state of the remote computer system (see Schneck column 4 line 66 – column 6 line 29 and column 7 line 55 – column 9 line 12).

With respect to claim 6, wherein, while the remote computer system is in a relatively high-security state, prior to loading and/or executing an untrusted software program into memory, the remote computer system sends a going-insecure message to the monitor (see Schneck figure 3 and column 7 line 55 – column 9 line 12), encrypted with a current key extracted from the data-storage medium local to the remote computer system (see Jones Abstract).

With respect to claim 7, wherein the monitor receives the going-insecure message, decrypts the initial-authentication message using a current key extracted from the data-storage medium local to the monitor (see Jones Abstract), and stores an indication that the remote computer system is in a relatively low-security state (see Schneck column 4 line 66 – column 5 line 24, column 7 line 55 – column 9 line 12 and column 10 line 26 – 67).

With respect to claim 8, wherein the data-storage media both contain identical sequences of encryption keys, and each of the data-storage media are one of: a

compact disc; a DVD disc; an electronic memory; and a magnetic disk (see figure 1 element 23 and 27 and abstract).

With respect to claim 9, a method for monitoring and reporting the security state of a remote computer system, the method comprising: providing a monitor computing device (see Schneck figure 1 element 106 Receive Host) interconnected with the remote computer system (see Schneck figure 1 element 103 Send Host) by a communications medium (see Schneck column 4 line 66 – column 5 line 24, column 7 line 55 – column 9 line 12 and column 10 line 26 – 67); and receiving messages from the remote computer system over the communications medium by the monitor and storing an indication, by the monitor, of the security state of the remote computer system determined by the monitor from the received messages (see Schneck column 4 line 66 – column 5 line 24, column 7 line 55 – column 9 line 12 and column 10 line 26 – 67). Schneck does not teach providing a pair of data-storage media, each containing a sequence of encryption keys, one data-storage medium local to the monitor computing device, and the other data-storage medium local to the remote computer system. Jones providing a pair of data-storage media, each containing a sequence of encryption keys, one data-storage medium local to the monitor computing device, and the other data-storage medium local to the remote computer system (see Jones abstract). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have a pseudo-random number generator at the transmitting and receiving stations to supply a like sequence of encryption keys to both the encryptor and decryptor, without these keys being

transmitted in any form over the transmission facility. Therefore one would have been motivated to have a pseudo-random number generator at the transmitting and receiving stations to supply a like sequence of encryption keys to both the encryptor and decryptor (see column 1 lines 37-53).

With respect to claim 10, further including receiving, by the monitor, a request for information about the security state of the remote computer system, and replying with a security-status-inquiry-response message by the monitor based on a determined security state of the remote computer system (see Schneck column 4 line 66 – column 5 line 24, column 7 line 55 – column 9 line 12 and column 10 line 26 – 67).

With respect to claim 11, further including, following power on or reset of the remote computer system, while the remote computer system is in a relatively high-security state, sending, by the remote computer system, an initial-authentication message to the monitor (see Schneck column 4 line 66 – column 5 line 24, column 7 line 55 – column 9 line 12 and column 10 line 26 – 67), encrypted with a next key extracted from the data-storage medium local to the remote computer system (see Jones abstract).

With respect to claim 12, further including receiving, by the monitor, the initial-authentication message, decrypting the initial-authentication message using a next key extracted from the data-storage medium local to the monitor, and storing an indication that the remote computer system is in a relatively high-security state (see Schneck column 4 line 66 – column 5 line 24, column 7 line 55 – column 9 line 12 and column 10 line 26 – 67).

With respect to claim 13, further including collecting, by the remote computer system, security metrics and including the security metrics in the initial-authentication message (see Schneck column 4 line 66 – column 5 line 24, column 7 line 55 – column 9 line 12 and column 10 line 26 – 67).

With respect to claim 14, further including receiving, by the monitor, the initial-authentication message and extracting the security metrics in order to determine the security state of the remote computer system (see Schneck column 4 line 66 – column 5 line 24, column 7 line 55 – column 9 line 12 and column 10 line 26 – 67).

With respect to claim 15, further including sending, by the remote computer system, a going-insecure message to the monitor, encrypted with a current key extracted from the data-storage medium local to the remote computer system, while the remote computer system is in a relatively high-security state, prior to loading and/or executing an untrusted software program into memory (see Schneck column 4 line 66 – column 5 line 24, column 7 line 55 – column 9 line 12 and column 10 line 26 – 67).

With respect to claim 16, further including receiving, by the monitor, the going-insecure message, decrypting the going-insecure message using a current key extracted from the data-storage medium local to the monitor, and storing an indication that the remote computer system is in a relatively low-security state (see Schneck column 4 line 66 – column 5 line 24, column 7 line 55 – column 9 line 12 and column 10 line 26 – 67).

With respect to claim 17, a computer instructions implementing the method of claim 9 encoded in a computer-readable medium (see Schneck column 3 lines 6-18).

With respect to claim 18, a monitor that monitors the security state of a computer system by the method of claim 9 (see Schneck column 4 line 66 – column 5 line 24, column 7 line 55 – column 9 line 12 and column 10 line 26 – 67).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

Application/Control Number:
10/693,182
Art Unit: 2132

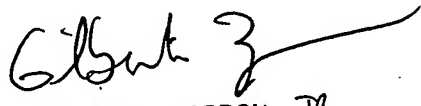
Page 10

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DA

Devin Almeida
Patent Examiner
12/3/2007


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100